PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30 | A1

(11) International Publication Number: WO 99/17496

(43) International Publication Date: 8 April 1999 (08.04.99)

(21) International Application Number: PCT/IL98/00474

(22) International Filing Date: 28 September 1998 (28.09.98)

(30) Priority Data:
121876 30 September 1997 (30.09.97) IL

(71) Applicant *(for all designated States except US)*: ALIROO LTD. [IL/IL]; Trumpeldor Street 19, 44442 Kfar Sava (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: POMERANTZ, Itzhak [IL/IL]; Golomb Street 18, 44357 Kfar Sava (IL). ZOREA, Meir [IL/IL]; Herzog Street 33, 76310 Rehovot (IL). COHEN, Ram [IL/IL]; Bartenura Street 13, Tel Aviv (IL).

(74) Agents: SANFORD, T., Colb et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

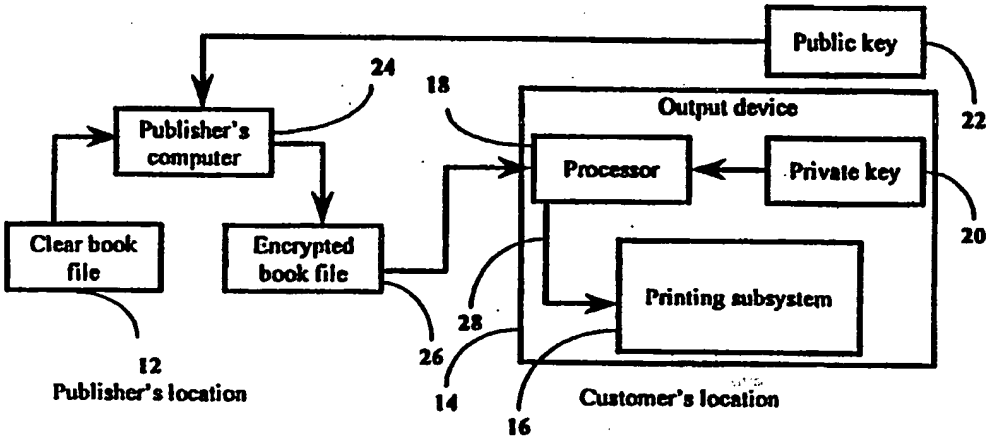
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ELECTRONIC PUBLISHING



(57) Abstract

This application discloses a method for restricted electronic transmission of information including the steps of encrypting information (#26) using a public key portion (#22) of a private/public key, transmitting the information following encrypting thereof over a medium which may be non-secure, receiving the information, following transmission thereof, at an output device (#14) in encrypted form, decrypting the information, received in encrypted form, at the output device using a private key portion (#20) of the private/public key, and following decryption in the output device, outputting the information (#28) in non-encrypted form. A system for restricted electronic transmission of information is also disclosed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

ELECTRONIC PUBLISHING

FIELD OF THE INVENTION

The present invention relates to publishing and more particularly to electronic publishing.

BACKGROUND OF THE INVENTION

Electronic publishing which has seen a substantial increase in popularity with the advent of the Internet, has encountered a serious problem of unauthorized publication over the Internet. Although copyright laws prohibit such unauthorized publications and downloads, in practicality, it is impossible to enforce copyright effectively in respect of a work which has been published on the Internet for unrestricted download.

Various techniques have been proposed for protecting electronically published materials. One example of such a technique appears in U.S. Patent 5,509,074 entitled "Method of protecting electronically published materials using cryptographic protocols". U.S. Patent 5,509,074 describes two alternative techniques for restricting the printing or display of electronically distributed publications.

A first technique calls for encryption and decryption using a secret key that is known only to the publisher and is also embedded in the printer or other output device. This technique has the disadvantage that it requires that each publisher transmit to a single printer or other output devices or that multiple publishers seeking to transmit to the same printer or other output device share a single secret key.

The second technique uses the secret key to convert the published material to a decrypted, bit-mapped representation of the material which includes information enabling the decrypted representation to be traceable to a user. This second technique has the disadvantage that it provides inadequate security, since bit-mapped representations may be reconverted into clean unencrypted form using conventional OCR techniques and the traceability can thus be defeated.

SUMMARY OF THE INVENTION

The present invention seeks to provide a method and system for providing secure electronic publishing which overcome limitations of the prior art.

There is thus provided in accordance with a preferred embodiment of the present invention a method for restricted electronic transmission of information including the steps of encrypting information using a public key portion of a private/public key, transmitting the information following encrypting thereof over a medium which may be non-secure; receiving the information, following transmission thereof, at an output device in encrypted form; decrypting the information, received in encrypted form, at the output device using a private key portion of the private/public key; and following decryption in the output device, outputting the information in non-encrypted form.

There is also provided in accordance with a preferred embodiment of the present invention a method for restricted electronic transmission of information including the steps of encrypting information, transmitting the information following encrypting thereof over a medium which may be non-secure; receiving the information, following transmission thereof in encrypted form, at a computer which is only able to decrypt the information when that computer is connected to a specific output device; decrypting the information, received in encrypted form, at the computer when connected to the specific output device; and following decryption, outputting the information in non-encrypted form at the output device.

Alternatively or additionally, decryption of the encrypted information at the computer connected to the specific output device is enabled by a preliminary decryption of the encrypted information by a secret key that is delivered to the computer subsequently to the transmission of the information.

Preferably the encrypting step includes two encryption steps, one encryption step using a public key and another encryption step using a secret key and wherein the decrypting step includes two decryption steps, one decryption step using the secret key and the other decryption step using a private key embedded in the output device and corresponding to the public key.

The secret key may be transmitted prior to, during or subsequently to the transmitting step.

Preferably, there is also provided the step of selectably formatting the information before or after the first decryption step and prior to the second decryption step.

In accordance with a preferred embodiment of the present invention, the another encryption step includes a plurality of separate encryption steps for separate portions of the information.

There is also provided in accordance with a preferred embodiment of the present invention a system for restricted electronic transmission of information comprising:

a public key encryptor, encrypting information using a public key portion of a private/public key;

an information transmitter, transmitting the information following encrypting thereof over a medium which may be non-secure;

a customer site receiver, remote from the encryptor, receiving the information, following transmission thereof, at an output device in encrypted form;

a decryptor, decrypting the information, received in encrypted form, at the output device using a private key portion of the private/public key.

There is additionally provided in accordance with a preferred embodiment of the present invention a system for restricted electronic transmission of information comprising:

an encryptor for encrypting information;

a transmitter, transmitting the information following encrypting thereof over a medium which may be non-secure;

a receiver, remote from the encryptor, receiving the information, following transmission thereof in encrypted form, at a computer which is only able to decrypt the information when that computer is connected to a specific output device; and

a decryptor, decrypting the information, received in encrypted form, at the computer when connected to the specific output device.

Preferably, the encryptor is operative to carry out two encryption steps, one encryption step using a public key and another encryption step using a secret key and wherein the decryptor is operative to carry out two decryption steps, one decryption step

using the secret key and the other decryption step using a private key embedded in the output device and corresponding to the public key.

In accordance with a preferred embodiment of the invention, there is also provided a computer for selectably formatting the information prior to decrypting thereof.

There is preferably also provided a customer site unit useful in any of the methods or systems described above and including an output device having embedded therein the private key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified functional block diagram illustration of a method and system for restricted electronic transmission of information constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified functional block diagram illustration of an alternative method and system for restricted electronic transmission of information constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 3A, 3B, 3C, 3D and 3E are illustrations of one mode of operation of the method and system of Figs. 1 & 2;

Fig. 4 is a simplified functional block diagram illustration of another method and system for restricted electronic transmission of information constructed and operative in accordance with a preferred embodiment of the present invention; and

Figs. 5A, 5B, 5C, 5D and 5E are illustrations of the operation of the method and system of any of Figs. 1 - 4 in accordance with another embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1, which is a simplified functional block diagram illustration of a method and system for restricted electronic transmission of information constructed and operative in accordance with a preferred embodiment of the present invention.

In the embodiment of Fig. 1, a clear, ready-for-print information file, such as a book file 12, in a standard file format, such as Postscript or PDF, is stored in a publisher's database. An output device 14, located at a customer's premises, remote from the publisher, typically includes a printing subsystem 16, such as a postscript HP Laser Jet printer and a processor 18, which may be a personal computer or any other suitable processor, or processor functionality which is incorporated in a processor present in the printing subsystem 16.

A private key 20, forming part of a private/public key encryption/decryption system, such as that available from RSA Inc. and described at www.rsa.com, is embedded in the output device 14, in a manner such that it cannot be accessed by any user, including the customer. The private key 20 is preferably embedded in the printing subsystem, but may alternatively be embedded in any other suitable portion of the output device 14.

In accordance with an alternative embodiment of the present invention, the printing subsystem 16 may be replaced by any other suitable type of output subsystem, such as a viewing subsystem, such as a display, or an audio annunciator subsystem, such as a speech generator. As a further alternative, the output device 14 may include more than one output subsystem of the type described hereinabove.

Associated with the private key embedded in the output device is a known public key 22 which is typically specified on the output device 14 or available on machine readable media. Alternatively or additionally, the public key 22 may be made readily available, i.e. as through posting on the Internet, to anyone who enters the serial number of the output subsystem, such as a printer.

When a customer wishes to order an electronic copy of a book or other information, the customer places an order with the publisher or the publisher's distributor. The order normally includes the standard billing information, such as a credit card number and a signature and the public key or information, such as the serial number of the printer, enabling the publisher to readily obtain the public key.

The publisher, using a computer 24, encrypts the clear file 12, using the public key and a conventional encryption engine which is commercially available from RSA Inc., thus providing an encrypted file 26. The encrypted file is communicated to the customer's

output device 14 via E-mail, FTP or any other suitable media, which may not be secure and is received at processor 18. The processor employs the embedded private key 20 to decrypt the received encrypted file and then sends the decrypted information via the internal circuitry 28 of the output device 14 to the printing subsystem 16 and/or other output subsystem for output to the customer. It is appreciated that the circuitry 28 must be secure from customer access in order to preserve security.

Reference is now made to Fig. 2, which is a simplified functional block diagram illustration of an alternative method and system for restricted electronic transmission of information constructed and operative in accordance with a preferred embodiment of the present invention. The embodiment of Fig. 2 is similar to that of Fig. 1, except in that the public key 22 is not transmitted by the customer to the publisher. Instead, the serial number 30 of the output device 14 or of the output subsystem 16 is transmitted via circuitry 36 and used to find the public key in a public key director 32. The remainder of the system and method of Fig. 2 is identical to that of Fig. 1.

In accordance with another embodiment of the present invention, the methods and systems of Figs. 1 and 2 may be operated so as to provide double encryption of the file 12. In addition to the encryption described hereinabove, the file may be encrypted additionally using a random symmetrical key selected by the publisher and kept secret by the publisher. The double encrypted file is then transmitted to the customer who cannot use it until he receives from the publisher, the secret second key used in the second encryption.

When the customer completes a purchase transaction, which may take place following transmittal of the file to the customer, the publisher communicates the secret second key to the customer, enabling him to decrypt the second encryption, typically using an ordinary computer which is used for receiving the encrypted file and is external to the output device. That computer will then send the decrypted information to the processor 18 of the output device, for the second decryption.

The methodology described hereinabove may be visualized by reference to Figs. 3A, 3B, 3C, 3D and 3E. Fig. 3A illustrates the clear file, here designated 42, Fig. 3B shows a first encryption 44, typically using the public key as described in hereinabove with reference to Figs. 1 & 2. Fig. 3C shows a second encryption 46. Upon carrying out

of the first decryption, typically in an ordinary PC that is external to the output device, the remaining file is still encrypted with the public key as shown in Fig. 3D. Upon further decryption using the private key, a clean file is provided, as seen in Fig. 3E.

Reference is now made to Fig. 4, which is a simplified functional block diagram illustration of another method and system for restricted electronic transmission of information constructed and operative in accordance with a preferred embodiment of the present invention;

The method and system of Fig. 4 may be similar to that of Fig. 2 at the publisher side, except that the first encryption is done with a symmetric key that is provided by the customer upon ordering, and not with a public key, and the second encryption is done with a random symmetric key that is unknown at the customer side. On the customer side, in the embodiment of Fig. 4, the output device 56 may be any conventional output device, and does not require any hardware modification whatsoever, provided that the output device has the facility of being able to communicate its serial number upon interrogation by a computer coupled thereto. This feature is now conventional in various printers, such as HP LaserJet series 5 printers available from Hewlett-Packard.

The customer may employ, for the first decryption of the decrypted information (stepping from Fig. 3C to Fig. 3D) and for formatting the encrypted information, a conventional PC including a display 52 and a processor and printer driver 54.

One of the present inventors has developed a technique whereby formatted alphanumeric text, such as RTF test in Windows, can be encrypted in such a way that the encrypted text preserves the format and text attributes of the original text. This technique is described and claimed in PCT Application PCT/IL96/00088, filed August 26, 1996, published as WO 97/09817 on March 1, 1997, the disclosure of which is hereby incorporated by reference.

It is appreciated that both the first and the second encryptions can be done while preserving the format of the original text. Moreover, the encrypted text can be reformatted while being encrypted, changing margins, line separations, font type and font size, for example. If a publisher chooses to encrypt the text in a way that preserves its format, then the customer can reformat the text to its needs without decrypting it, thus preparing it for printing in a desired format.

When a customer wishes to order an electronic copy of a book or other information, the customer places an order with the publisher or the publisher's distributor. The order normally includes the standard billing information, such as a credit card number and a signature and the serial number of the output device, the printer or other output subsystem. The encryption is carried out by any suitable file encryption software using a key that does not have to be secret, inasmuch as the key is not sufficient for decryption. A preferred file and text encryption software package is commercially available from Aliroo Ltd. of Israel under the trademark PrivaSuite.

The publisher, using a computer 54, encrypts the clear file 62. The encryption is carried out by any suitable file encryption software using a key that does not have to be secret, inasmuch as the key is not sufficient for decryption. A preferred file encryption software package is commercially available from Aliroo Ltd. of Israel under the trademark PrivaSuite. The encrypted file 66 is communicated via E-mail, FTP or any other suitable media, to the customer's computer 68, where it can be reformatted and decrypted and sent to the output device 50.

The processor 68 polls the output device 56 for the known serial number thereof or for a secret serial number that is embedded therein and uses that number to decrypt the file using suitable decryption software, preferably PrivaSuite. The decrypting software does not accept the decryption key from any source other than a serial number reported by the output device 50.

In accordance with a preferred embodiment of the present invention, the output device 50 includes a built-in software protection dongle 70, such as a dongle commercially available from Aladdin or Micro-Macro, which is logically interconnected between the processor 68 and the output subsystem.

The embodiment of Fig. 4 has the advantage that it enables the received information to be displayed on the screen and formatted by a customer, using standard formatting software such as Acrobat by Adobe, in order to determine the font size, the pages to be printed, the margins and similar parameters. Printing of the information is only permitted by means of the print driver which is written to send the file only to a printer that suitably identifies itself and, if a dongle is provided, presents the dongle key which corresponds to the printer.

The embodiment of Fig. 4 does not require any change in the design of the printer but does have a cryptographic weakness in that the output connection from the processor and printer driver, indicated by reference numeral 84 is accessible. If the data can be recorded from the output connection 84, the cryptographic protection is overcome.

Reference is now made to Figs. 5A, 5B, 5C, 5D and 5E which are illustrations of operation of the method and system of any of Figs. 1 - 4 in accordance with an additional embodiment of the present invention. A document 88 is shown to have a table of contents 90 and typically three chapters, A, B and C, indicated by respective reference numerals 92, 94 and 96. The document can be distributed and licensed in accordance with any of the methods described above and using any of the systems described hereinabove.

Thus, each of chapters A, B and C can be identically encrypted as by the publisher's computer 12 (Fig. 1) with a public key as described hereinabove. The thus encrypted file, wherein a portion thereof, such as the table of contents 90 is typically not encrypted, is shown at reference numeral 100. This encryption is illustrated by frames 102 formed about each of chapters 92, 94 and 96.

If it is desired to separately license each of the chapters A, B and C, each chapter can be separately encrypted, as with a symmetric secret key, in much the same manner as described hereinabove with reference to Figs. 3A - 3E. The double encrypted file is indicated by reference numeral 104 and preferably includes an unencrypted table of contents 90. The separate encryptions are indicated by respective frames 106, 108 and 110 surrounding frames 102. The secret keys for the second encryption are stored in the publisher's data base and are transmitted to the customer, as and when the customer purchases a given chapter.

Decryption of the individual chapters using the secret keys and using the private key take place as illustrated in Figs. 5D and 5E.

It is appreciated that the double encryption functionality shown in Figs. 3A - 3E and 5A - 5E enables transmission of the information to be decoupled from licensing thereof, so as to enable transmission to occur when convenient and cost effective and licensing to occur at a time convenient to the customer.

It will be apparent to persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and sub-combinations of the features described hereinabove as well as modifications and further developments thereof which would occur to a person of skill in the art upon reading the foregoing description, which are not in the prior art.

CLAIMS

1. A method for restricted electronic transmission of information including the steps of:

encrypting information using a public key portion of a private/public key;

transmitting the information following encrypting thereof over a medium which may be non-secure;

receiving the information, following transmission thereof, at an output device in encrypted form;

decrypting the information, received in encrypted form, at the output device using a private key portion of the private/public key; and

following decryption in the output device, outputting the information in non-encrypted form.

2. A method for restricted electronic transmission of information including the steps of:

encrypting information;

transmitting the information following encrypting thereof over a medium which may be non-secure;

receiving the information, following transmission thereof in encrypted form, at a computer which is only able to decrypt the information when that computer is connected to a specific output device;

decrypting the information, received in encrypted form, at the computer when connected to the specific output device; and

following decryption, outputting the information in non-encrypted form at the output device.

3. A method according to either of claims 1 and 2 and wherein the encrypting step includes two encryption steps, one encryption step using a public key and another encryption step using a secret key and wherein the decrypting step includes two

decryption steps, one decryption step using the secret key and the other decryption step using a private key embedded in the output device and corresponding to the public key.

4. A method according to claim 3 and wherein the secret key is transmitted prior to the transmitting step.

5. A method according to claim 3 and wherein the secret key is transmitted during the transmitting step.

6. A method according to claim 3 and wherein the secret key is transmitted following the transmitting step.

7. A method according to any of the preceding claims and also comprising the step of selectably formatting the information prior to decrypting thereof.

8. A method according to claim 3 and wherein the another encryption step includes a plurality of separate encryption steps for separate portions of the information.

9. A system for restricted electronic transmission of information comprising:

a public key encryptor, encrypting information using a public key portion of a private/public key;

an information transmitter, transmitting the information following encrypting thereof over a medium which may be non-secure;

a customer site receiver, remote from the encryptor, receiving the information, following transmission thereof, at an output device in encrypted form;

a decryptor, decrypting the information, received in encrypted form, at the output device using a private key portion of the private/public key.

10. A system for restricted electronic transmission of information comprising:

an encryptor for encrypting information;

a transmitter, transmitting the information following encrypting thereof over a medium which may be non-secure;

a receiver, remote from the encryptor, receiving the information, following transmission thereof in encrypted form, at a computer which is only able to decrypt the information when that computer is connected to a specific output device; and

a decryptor, decrypting the information, received in encrypted form, at the computer when connected to the specific output device.

11. A system according to either of claims 9 and 10 and wherein the encryptor is operative to carry out two encryption steps, one encryption step using a public key and another encryption step using a secret key and wherein the decryptor is operative to carry out two decryption steps, one decryption step using the secret key and the other decryption step using a private key embedded in the output device and corresponding to the public key.

12. A system according to claim 11 and wherein the secret key is transmitted prior to the transmitting step.

13. A system according to claim 11 and wherein the secret key is transmitted during the transmitting step.

14. A system according to claim 11 and wherein the secret key is transmitted following the transmitting step.

15. A system according to any of the preceding claims 9 - 14 and also comprising the a computer for selectably formatting the information prior to decrypting thereof.

16. A system according to claim 11 and wherein the another encryption step includes a plurality of separate encryption steps for separate portions of the information.

17. A customer site unit useful in a method according to any of claims 1 - 8 and including an output device having embedded therein the private key.

18. A customer site unit useful as part of a system according to any of claims 9 - 16 and including an output device having embedded therein the private key.

19. A customer site unit useful as part of a system according to any of claims 9 - 16 and also including a software dongle.

20. A system according to any of claims 9 - 10 and also comprising a software dongle in said output device.

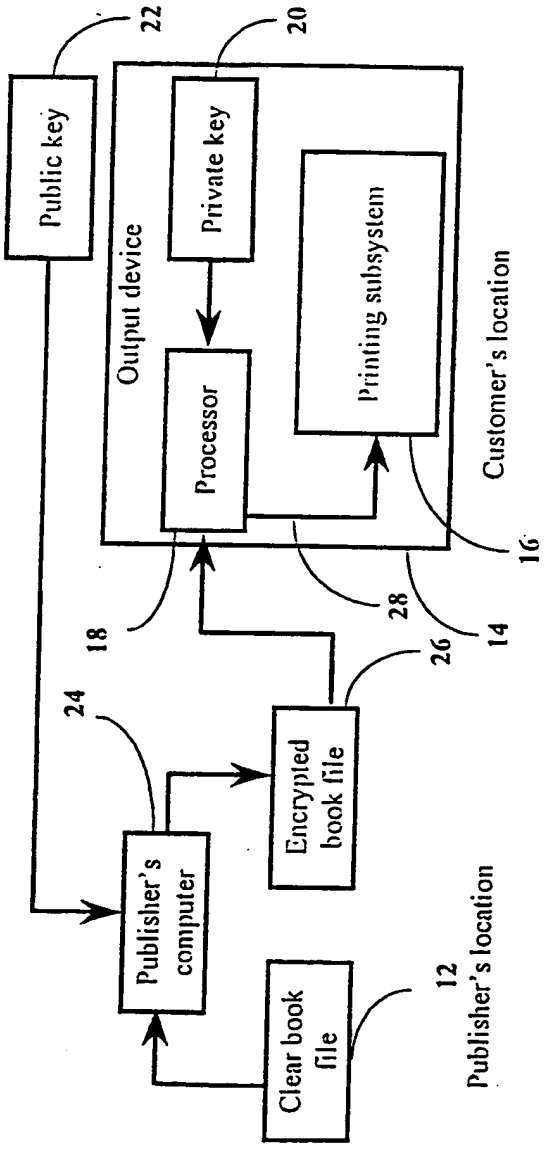

Public key
22
20
Private key
Output device
Printing subsystem
Processor
Customer's location
16
18
28
14
26
24
Encrypted book file
Publisher's computer
Clear book file
12
Publisher's location

Fig. 1

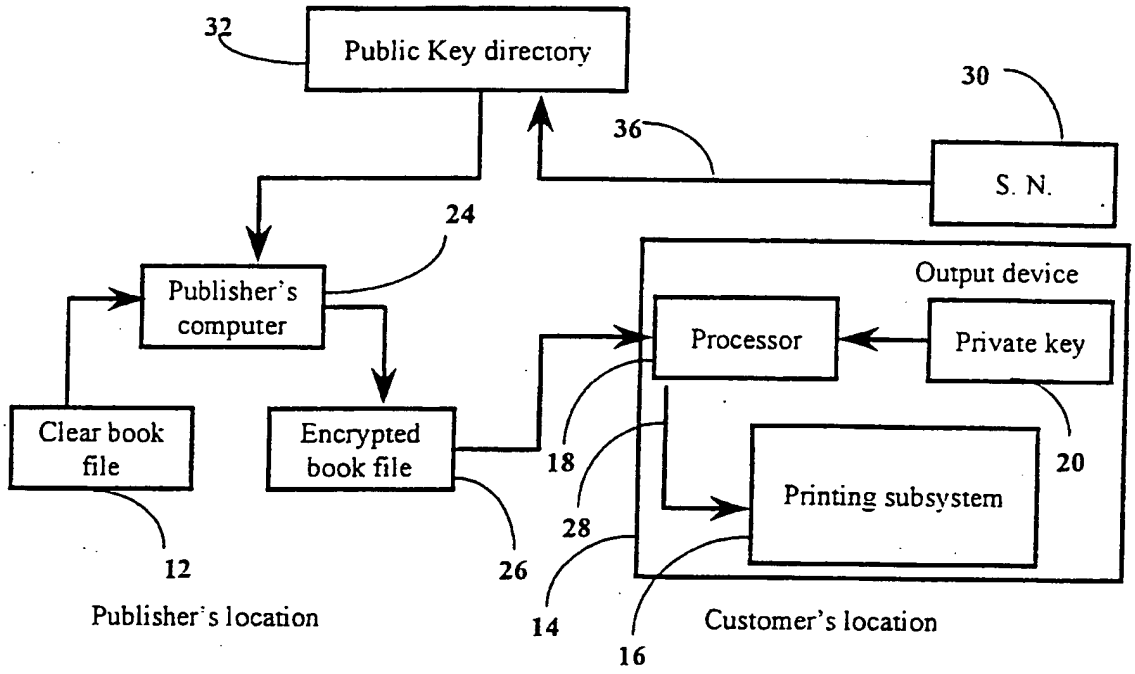


Fig. 2

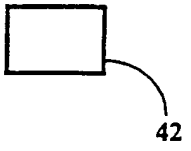


Fig. 3A

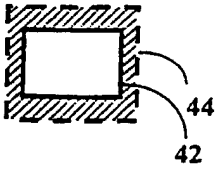


Fig. 3B

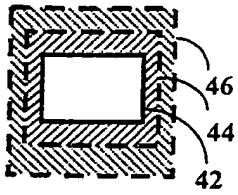


Fig. 3C

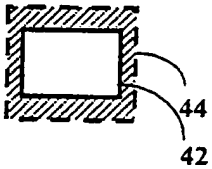


Fig. 3D

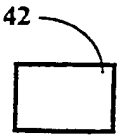


Fig. 3E

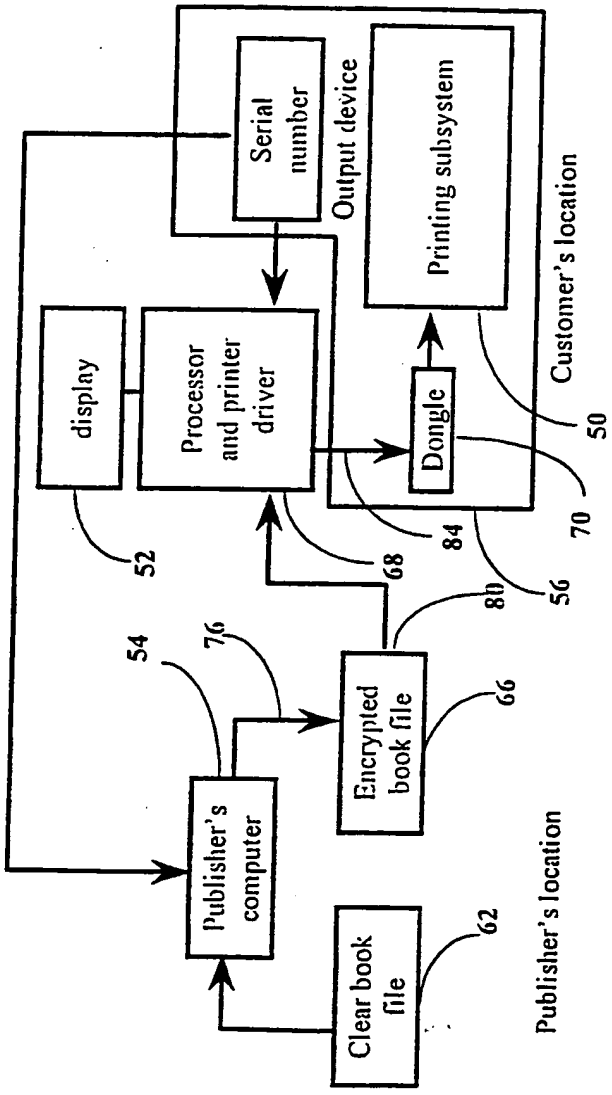

Serial number
Output device
Printing subsystem
Customer's location
display
Processor and printer driver
Dongle
50
52
68
84
70
56
80
54
76
Encrypted book file
66
Publisher's computer
Clear book file
62
Publisher's location

Fig. 4

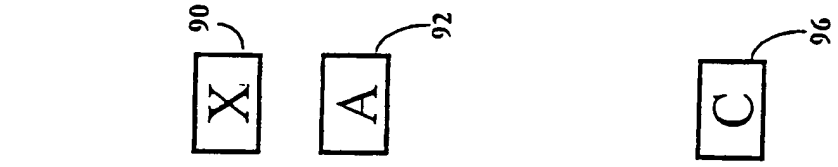


Fig. 5E

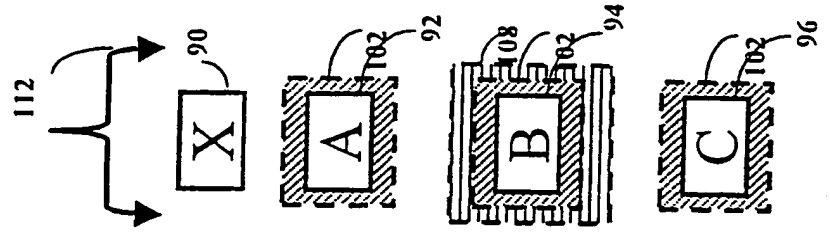


Fig. 5D

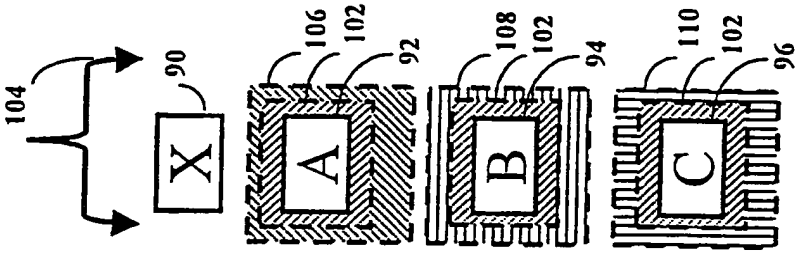


Fig. 5C

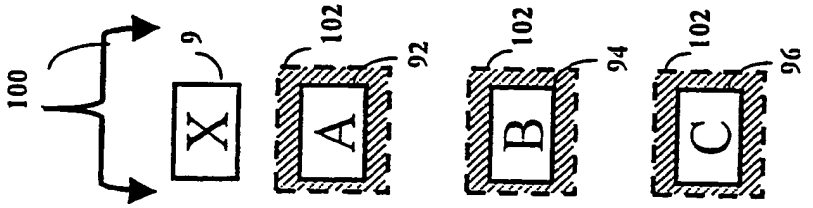


Fig. 5B

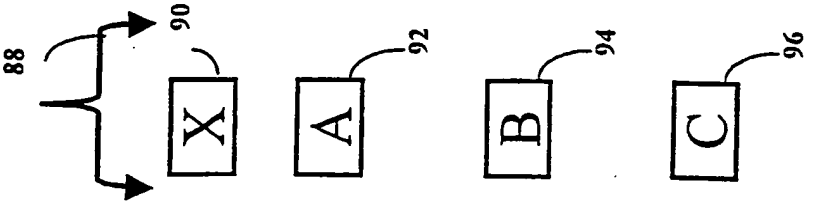


Fig. 5A

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00474

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H 04 L 9/30
US CL :380/21,30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/21,30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS
search terms: public key, dongle, transmission, sending, information, message, network

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,142,579 A (ANDERSON) 25 AUGUST 1992 (25.08.92), abstract, fig.1, column 3, lines 60-68, column 4, lines 1-20.	1-16
---		-----
Y		20
Y	US 5,377,268 A (HUNTER) 27 December 1994 (27.12.94), column 9, lines 56-68.	20
A	US 5,150,411 A (Maurer) 22 September 1992 (22.09.92), column 5, lines 32-61.	1-16
A,P	US 5,761,305 A (VANSTONE et al.) 02 June 1998 (02.06.98), column 3, lines 33-59, column 4, lines 22-25, column 6, lines 57-63.	1-16
A	US 5,568,554 A (EASTLAKE, 3rd) 22 October 1996 (22.03.96), abstract, fig.1, column 4, lines 10-43.	1-16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
18 DECEMBER 1998

Date of mailing of the international search report
11 MAR 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
GAIL HAYES
Telephone No. (703) 305-9711

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00474

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 17,18,19
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.